Solutions II
Security Services Catalog

2017

Version 2.8
# Table of Contents

- Introduction .................................................................................................................. 3
- Overview ....................................................................................................................... 3
- Services Summary ......................................................................................................... 4
- Security Services ......................................................................................................... 5
  - Security Professional Services .................................................................................. 6
  - Security Assessment ................................................................................................. 6
  - Risk and Compliance ............................................................................................... 7
  - Incident Response ..................................................................................................... 8
- Security Advisory ......................................................................................................... 8
- Security Managed Services .......................................................................................... 9
  - Security Monitoring and Alerting ............................................................................ 9
  - Threat Intelligence .................................................................................................... 9
  - Security Device Management .................................................................................. 10
  - Incident Response ................................................................................................... 10
Introduction
This catalog provides an overview of our Services Portfolio outlining the benefits that can be delivered to our clients.

For more than 25 years, Solutions II has delivered outstanding services to our clients using our services methodology. We maintain numerous vendor certifications coupled with hands-on experience which allows us to design, deploy, document and manage those multi-vendor environments.

Our clients leverage our expertise and solutions to lower their IT capital and operating costs. With the fast changing IT world, your team can use us to navigate the ever-changing technologies allowing you to overcome financial constraints and limited internal IT knowledge and focus directly on your core business objectives.

Overview
Solutions II is nationally recognized as a comprehensive Infrastructure as a Service (IaaS) Provider, empowering our client’s business models through a seamless delivery of a full suite of Professional and Managed IT Services. Solutions II’s commitment of bringing best-of-breed solutions to clients includes a professional services practice dedicated to increasing customer service levels and decreasing the time and support required for implementations to keep their clients “Performing Ahead of the Curve.”

Service Portfolio Offerings Across Multiple Platforms whether “on prem” or “cloud based”
• Architectural Services
• Professional Services
• Managed Services

Why Solutions II Services?
• Depth of Experience and Expertise
  Access to subject matter experts with 200+ technical certifications that design and deliver your solution.

• Breadth of Services Suite
  Network, security, cloud, virtualization, business continuance and data optimization combine make us a one-stop comprehensive Service Provider.

• Reliability and Consistency Client Outcomes
  Our goal is to build trust through a commitment to team, partnership and success by delivering projects on time and under budget.

• Account Support Including Client Account Management
  Clients consider us an extension of their team. We demonstrate teamwork through collaborative efforts like industry leading documentation, assessments, business impact analysis, on-time project management and quarterly business reviews.
Services Summary

Since 1992, Solutions II has a proven track record of delivering outstanding services to our clients with our fully developed services methodology. Our services organization maintains numerous vendor certifications with hands-on experience that allows us to design, deploy, document and manage those complex multi-vendor environments.

• Solution Design
• Consulting Services
• Assessments
• Strategy & Optimization

• Assessments
• Implementation
• Migrations
• Project Management
• Staff Augmentation

• Data Center
• Backup and Recovery
• Network
• Voice
• Power i
• Service Desk

• Assessments
• Risk & Compliance
• Incident Response
• Advisory
• Managed Services

• Public Cloud
• Private Cloud
• Secure Cloud
• Hybrid Cloud
• Cloud Storage

• Microsoft Consulting Services
• Post Warranty Maintenance
• Data Erasure Services

Breadth of Services Suite

Solutions II is a one-stop comprehensive Service Provider. We have practice areas in networking, security and cloud, virtualization, business continuance and data optimization.

Experience and Expertise

Access to subject matter experts with 200+ technical certifications that design and deliver your solution.

Reliability and Consistency

Our goal is to build trust through a commitment to team, partnership and success by delivering projects on time and within budget.

Account Support Including Client Account Management

Solutions II is considered by our clients as an extension of their team. We demonstrate teamwork through collaborative efforts like industry leading documentation, assessments, business impact analysis, on-time project management and more!
Security Services

In today’s information technology world, it is of the utmost importance to proactively manage your organization’s information security to mitigate risks to your most important assets and to your overall business. Your organization stores intellectual property, trade secrets, financial data, employee and customer data. It is imperative you maintain confidentiality, integrity and availability of these assets should be the highest priority of every organization. Leveraging Solutions II Security Services will help manage risks to your IT assets in a secure, efficient, cost-effective manner aligned with industry best practices.

At Solutions II, we help organizations manage their IT security through a variety of professional and managed services that provide high value and peace of mind. Our Security Services are designed to help organizations secure their critical assets while saving money and freeing up resources, so that you can focus on the core of your organization, alleviating the worry and risk.

Benefits / Highlights
- Clear Understanding of Client’s Business Requirements
- Architect Comprehensive Solutions
- Deliver Security Solutions Involving Infrastructure System Architecture and Design
- Ability to Solve Specific Client Security Problems
- Improve Risk Management
- Enhance Operational Efficiencies, Security and Compliance

Services Offered:
- **Professional Services**
  - Assessments
  - Risk and Compliance
  - Incident Response
  - Security Advisory
- **Managed Services**
  - Security Monitoring and Alerting
  - Threat Intelligence
  - Security Device Management
  - Incident Response

YOUR DATA IS YOUR BUSINESS. SECURITY IS OURS.
Security Professional Services
Solutions II Security Professional Services will provide you with the experience and skills to protect and optimize all security and business stability issues while optimizing your spend. Our security professional services free up resources in your organization allowing you to concentrate on your core business and deliver competitive advantages. We provide independent advice, consulting and the expertise to address all your security requirements.

Security Assessment

**Red Team Services**: A complete security assessment offering that utilizes all security assessment services as one cohesive service. Information is utilized between all activities and is used to test your organization’s security defenses in a manner most consistent with adversarial actions.

**Vulnerability Management Program Gap Assessment**: A top-down review of your vulnerability management program from documentation to execution. Solutions II will review your organization’s Vulnerability Management Program documentation, interview personnel to evaluate processes, and perform internal and external network vulnerability and penetration testing activities to evaluate the effectiveness of the program.

**External Network Vulnerability and Validation Testing**: Discovery of externally available devices, ports/services, and vulnerabilities is performed from both manual and automated scanning. Vulnerabilities are manually validated to provide evidence of potential results and removal of false-positives.

**Internal Network Vulnerability and Validation Testing**: Discovery of internal devices, ports/services, and vulnerabilities is performed from both manual and automated scanning. Vulnerabilities are manually validated to provide evidence of potential results and removal of false-positives.

**Internal Network Vulnerability and Penetration Testing**: The addition of the penetration testing allows Solutions II consultants to engage client infrastructure in a similar fashion as an adversary. Attacking known vulnerabilities to gain access may then lead to lateral movement within the organization. End-Goals for penetration testing is defined by the client.

**Internal Application Security Testing**: Testing specifically focused on internally facing web and thin-client/thick-client applications. Automated and manual vulnerability and penetration testing performed on applications to ensure secure coding practices, communications, and configurations are utilized.

**External Application Security Testing**: Testing specifically focused on externally facing web applications. Automated and manual vulnerability and penetration testing performed on applications to ensure secure coding practices and web server configurations are utilized.

**External Network Vulnerability and Penetration Testing**: The addition of the penetration testing allows Solutions II consultants to engage client infrastructure in a similar fashion as an adversary. Attacking known vulnerabilities to gain access may then lead to lateral movement within the organization. End-Goals for penetration testing is defined by the client.

**Internal Application Security Testing**: Testing specifically focused on internally facing web and thin-client/thick-client applications. Automated and manual vulnerability and penetration testing performed on applications to ensure secure coding practices, communications, and configurations are utilized.

**Wireless Security Assessment**: Wireless configuration and security review of implemented wireless access points and infrastructure.

**Password Complexity Validation**: Solutions II performs password cracking attempts against client provided .dit file for purposes of identification of easy to guess or weak passwords.

**Device Security Testing**: Solutions II will perform assessment activities from both technical and physical perspectives on client provided devices. Devices are inspected to determine if attackers are able to gain access to sensitive data, modify devices, or perform other malicious actions towards the device and loaded software.
Personnel Security – Phishing: Email campaign(s) utilized to identify weaknesses in employee security awareness in regards to email reception and actions executed as requested in the campaign email.

Personnel Security – Social Engineering: Phone campaign(s) to identify weaknesses in employee security awareness in regards to actions performed and information provided during the campaign phone call.

Enterprise security risk assessment
We don’t just analyze security risks as they apply to specific systems. We look at your whole organization to evaluate your overarching security practices and deliver an exhaustive report detailing how you can improve your security policies. Threat mitigation begins with a solid foundation.

Risk and Compliance

PCI Gap Assessment: A review of client’s current PCI compliance stance through interviews, documentation review, and minimal controls validation.

PCI Audit: A complete PCI audit utilizing the latest released DSS version (currently 3.2) for auditing organizations PCI environment(s) for compliance against documented requirements.

HIPAA Gap Assessment: A review of current controls and gaps as compared to HIPAA requirements.

HIPAA Audit: A complete HIPAA audit.

ISO Gap Assessment: A review of current security gaps as compared to ISO 27001.

ISO Audit: A complete ISO 27001 audit.

FedRAMP Moderate: The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Our FedRAMP-compliant PaaS offers federal agencies secure cloud storage and solutions providing the highest degree of protection for vital government information.

NIST Gap Assessment: A gap review of an organizations security posture as it relates to NIST SP800-53 R4 and other NIST documentations.

CIS Top 20 CSC Gap Assessment: A gap review of an organizations current security controls against the Center for Internet Security 20 Critical Security Controls documentation.


Policy Audit: A review of documented polices compared against a variety of standards and compliance bodies.

FISMA (Low and Mid-Level): The Federal Information Security Management Act (FISMA) outlines security guidelines federal agencies must follow to protect confidential information. Because FISMA compliance is essential to securing the economic and national security interests of the United States government, we have created a FISMA-compliant solution that ensures a high level of security.

SSAE 16 SOC 2 Type II: The SSAE 16 represents more globally accepted accounting principles. SSAE compliance guarantees adequate controls are in place to protect personal client information. Our data centers are SSAE-16 SOC 2 certified and provide a broad range of physical security capabilities, providing a secure cloud environment that’s highly responsive.
Incident Response

Compromise Assessment: Identification service for the discovery of potential compromise within the organization. Analysis of data collected during the engagement focuses on malicious activities performed within the organization, malicious outbound connections, and malicious applications.

Incident Response Program Development: Solutions II will assist in developing an internal incident response program that utilizes current capabilities, development of increased internal skills and knowledge, solutions gap and remediation plans, and roadmap for program maturation.

Incident Response Gap Assessment: Solutions II will analyze the current people, processes, and technology of an organization as it pertains to each phase of the incident response life-cycle.

Incident Response Plan/Playbook Development: Solutions II will assist in developing organizational Incident Response documentation based off of interviews of pertinent personnel, review of controls in-place, and our experience in delivering Incident Response services.

Retainer: A defined block of pre-paid hours that may be utilized for incident response services.

Security Advisory

Virtual CISO (vCISO): Executive level services for development and/or maturation of an organization’s security posture from a leadership perspective.

Block of Advisory/Consulting Hours: Prepaid blocks of consulting hours to be utilized for delivery of pre-defined services.

INCIDENT RESPONSE PLAN? CHECK.
SLEEP BETTER AT NIGHT? CHECK.
Security Managed Services

At Solutions II our Security Managed Services organization will defend and protect your organization from increasingly sophisticated, sometimes daily cybercrime threats. We provide day-to-day security defenses of your technology infrastructure by monitoring your network, systems and data, 24 hours per day, 7 days a week, 365 days per year. This allows us to effectively secure your environment and if threats occur quickly identify, analyze and respond, giving you peace of mind.

Security Monitoring and Alerting

Solutions II’s security monitoring solutions are designed to complement your current IT resources, save your organization money, and provide you with peace of mind. Managed by our team of certified security analysts, our 24/7 security monitoring and alerting services identify threats, mitigate future issues, and provide in-depth reporting that gives you complete visibility of your organization’s data security. We work with you to achieve complete compliance under industry regulations like PCI DSS, GLBA, NERC, CIP, CJIS and HIPAA.

Our managed security monitoring and alerting service is designed to seamlessly integrate with your current business intelligence and analytics platforms to help you make better business decisions.

Solutions II’s security monitoring and alerting solutions feature:

- 24/7 Real-time Monitoring, Alerting and Analysis by Certified Security Analysts
- Integrated Business Intelligence and Analytics to Make Better Business Decisions
- Asset Classification and Reporting
- Flexible and Customizable Reporting
- Easy Integration with Existing Solutions and Workflow Products
- Pre-built Security and Compliance Reports

Threat Intelligence

Most organizations rely on legacy, signature-based intelligence feeds that provide a false sense of safety. These programs cannot help anticipate attacks or guide responses. They often simply increase alert volumes with false positives, wasting security analysts’ time, increasing the complexity of the security environment, and making attacks impossible to manage.

Cyber threat intelligence, when used correctly, can help defenders detect attacks during — and ideally before — a potentially damaging threat.

Solutions II’s Threat Intelligence solution gives us comprehensive view of the web and mobile frontiers. Through our partnership with RiskIQ, we are monitoring 9M+ websites and 141+ mobile app stores daily, adding more site and app store crawls continually.

In addition to detecting instances of malware and other online threats to an organization, Solutions II powered by RiskIQ enables our clients to create their own policies to detect instances that may bring the organization out of compliance. Multiple built-in and external enforcement options are available to mitigate or remediate incidents we discover.

Solutions II’s Threat Intelligence solution provides your organization capabilities that include web-scale crawling and analysis. We have been gathering data on malware, exploits, malvertisements, and mobile app stores since 2009, and this historical data allows our clients to proactively defend against threats to their customers and employees.
Security Device Management

Solutions II works with companies to increase the value of the infrastructure they have already heavily invested in. We aim to relieve the anxiety of your IT team by implementing security, incident and change management practices that ensure your security technology investment is being properly configured and tuned, by our team of certified experts.

Our partnerships with industry-leading security technology companies put Solutions II at the forefront of the device security industry. We actively work with our technology partners on development, implementing best practices and ensuring we are bringing a level of experience to the table that is simply impossible for organizations to match in-house.

We work closely with in-house teams to implement systems that allow organizations to focus on the core of their business, while we handle the device management. We can also provide a co-managed solution that allows Solutions II to work closely with your IT team through a common change management system and process. Our managed security device management solutions can help your organization with:

- Device Configuration and Tuning
- Updates and Patch Management
- Flexible SLAs to Match Client Needs
- Monitoring of Log Threat Detection
- 24/7 Escalation and Context-aware Alerting

Incident Response

Solutions II’s managed incident response service is designed to end attacks before they begin. When breaches do occur, we help companies implement procedures that thwart the attack, remove the source, and mitigate damage to your finances and reputation.

Our incident handlers have vast experience in incident response procedures in a wide variety of industries. We work closely with internal teams to provide guidance and direction that can mean the difference between a thwarted threat and a disaster for your organization. We work with your team through all phases of a security crisis to minimize the impact of the attack and put your organization in a position to recovery quickly, while taking steps to ensure that similar attacks are prevented in the future.

Our managed incident response service can help your organization:

- Stop the Attack
- Identify What Assets May Have Been Affected
- Collect All Relevant Evidence for Civil, Criminal or Regulatory Proceedings
- Remove the Source of the Breach
- Mitigate the Financial and Reputational Impact of the Breach
- Recommend and Implement Operational Improvements to Prevent Similar Breaches in the Future